*PATENT*

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | | |
|---|---|---|---|
| Appellants: | **Siani Lynne PEARSON et al.** | Examiner: | Andrew L. NALVEN |
| Serial No.: | **09/932,476** | Art Unit: | 2134 |
| Filed: | August 17, 2001 | Our Ref: | B-4279 619006-5<br>30006639-2US |
| For: | "TRUSTED SYSTEM" | Date: | March 27, 2007 |
| | | Re: | ***Appeal to the Board of Appeals*** |

## BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection dated December 26, 2006, for the above identified patent application. Please charge the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief to deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed because the Notice of Appeal was filed on January 30, 2007.

## REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

## CONCLUSION

In view of the extensive reasons advanced above, Appellant respectfully contends that each pending claim is in fact novel and patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

March 27, 2007
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)

(Signature)

3/27/07
(Date)

Attachments

Respectfully submitted,

Robert Popa
Attorney for Appellant
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

## RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

## STATUS OF CLAIMS

Claims 1-10 are the subject of this Appeal and are reproduced in the accompanying appendix. Claims 11-17 have been withdrawn.

## STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

## SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in claim 1 is directed to a method for allowing a financial transaction to be performed using a electronic system, the method comprising interrogating an electronic transaction terminal (10) with an electronic security device (19) to obtain an integrity metric for the transaction terminal measured by a trusted device (24) associated with the transaction terminal after the last restart of the transaction terminal (p. 6 l.4 – p. 14 l. 13); determining if the transaction terminal is a trusted terminal based upon the integrity metric (p.12 ll. 4-21); and allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal (p. 19 l .1 – p. 20 l. 5, Figs. 1-7).

The invention described and claimed in claim 5 is directed to a financial transaction system comprising an electronic financial transaction terminal (10); and an electronic security device (19) having interrogation means (67) for interrogating the transaction terminal to obtain an integrity metric for the transaction terminal measured by a trusted device (24) associated with the transaction terminal after the last restart of the transaction terminal (p. 6 l.4 – p. 14 l. 13), determining means (65) for determining if the transaction terminal is a trusted terminal based upon the integrity metric (p.12 ll. 4-21), and means (62) for allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal (p. 19 l .1 – p. 20 l. 5, Figs. 1-7).

The invention described and claimed in claim 8 is directed to a electronic security transaction device (19) having interrogation means (67) for interrogating an electronic financial transaction terminal to obtain an integrity metric for the transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal (p. 6 l.4 – p. 14 l. 13), determining means (65) for determining if the transaction terminal is a trusted terminal based upon the integrity metric (p.12 ll. 4-21), and means (62) for allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal (p. 19 l .1 – p. 20 l. 5, Figs. 3-5).

## GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-2, 4-5, 8 and 10 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 6,925,566 to Feigen (hereinafter "Feigen") in view of U.S. Pat. No. 5,794,054 to Le (hereinafter "Le") et al. and further in view of U.S. Patent No. 5,721,781 to Deo (hereinafter "Deo").

Issue 2: Whether claims 3 and 6 are patentable under 35 U.S.C. 103(a) over Feigen, Le and Deo and further in view of U.S. Patent No. 6,694,436 to Audebert (hereinafter "Audebert").

Issue 3: Whether claim 7 is patentable under 35 U.S.C. 103(a) over Feigen, Le, Deo and Audebert and further in view of U.S. Patent No. 6,772,331 to Hind (hereinafter "Hind").

Issue 4: Whether claim 9 is patentable under 35 U.S.C. 103(a) over Feigen, Le and Deo and further in view of U.S. Patent No. 5,272,754 to Boerbert (hereinafter "Boerbert").

## THE ARGUMENT

**Issue 1: Whether claims 1-2, 4-5, 8 and 10 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 6,925,566 to Feigen (hereinafter "Feigen") in view of U.S. Pat. No. 5,794,054 to Le (hereinafter "Le") et al. and further in view of U.S. Patent No. 5,721,781 to Deo (hereinafter "Deo").**

On page 4 of the Office Action of December 26, 2006, the Examiner rejects claims 1-2, 4-5, 8 and 10 under 35 U.S.C. 103(a) as being unpatentable over Feigen, Le and Deo. In particular (and *inter alia*), the Examiner finds that, with regard to claims 1, 5 and 8, Feigen teaches the interrogating of an electronic transaction terminal with an electronic security device

to obtain an in integrity metric for the transaction terminal at col. 2 ll. 29-48, and determining if the transaction terminal is a trusted terminal based upon the integrity metric. Appellants respectfully disagree.

In their previous submission, Appellants noted that the passage in Feigen cited to by the Examiner (reproduced below for ease of reference) does not in fact support the Examiner's position:

> After a decision has been made to verify the integrity of a particular remote unit, the verification unit identifies a memory range or ranges within the remote unit the contents of which are to be hashed. The verification unit also generates a random seed value that is to be planted within the data stream being hashed in the remote unit. In addition, the verification unit determines the location within the data stream at which the random seed value is to be placed. The verification unit then delivers an interrogation signal to the remote unit that includes the memory range information, the random seed value, and the random seed value location information. The interrogation signal is also delivered to the local communication unit. The remote unit and the local unit then each perform the requested hash operation and each return a hash value to the verification unit. The verification unit then compares the values to determine whether any modifications have occurred within the remote unit. If the values are not the same, the system determines that modifications have been made and further investigation is initiated.

As previously explained, a careful reading of the rest of Feigen reveals that the "verification unit" is actually located remotely from the remote unit (at the head-end) and thus

can in no way be understood to be "a trusted device associated with the transaction terminal." Thus, Appellants traversed the Examiner's characterization of Feigen as the alleged "integrity metric" obviously does not read upon the claimed integrity metric that is clearly recited in the claims as being measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal, and explained that they were therefore compelled to disagree that Feigen discloses the interrogation of a transaction terminal to obtain an integrity metric for the transaction terminal.

Presently the Examiner answers the above by asserting that "the word 'associated' can in no way be interpreted to be in close proximity" and concluding that, because the claims do not require that the electronic security device be in close proximity to the transaction terminal, Feigen's remote verification unit is within the scope of the broadest reasonable interpretation of the claims. Appellants once again respectfully disagree, and note at the outset that it is well-established precedent that claims should be read in light of the specification, just as limitations in the specification should not be read into the claims (*Liebel-Flarsheim Co. v Medrad, Inc.*, 358 F.3d 898, 904-905 (Fed. Cir. 2004). Thus, by following well-settled precedent and consulting – as a first step – the specification, the reader is informed that the claimed electronic security device (i.e. the platform 10) contains the trusted device (see, *e.g.*, p. 6 l. 4 of the present specification). Even consulting a dictionary would have informed the Examiner that the term associated can and indeed *should* be interpreted as being in close proximity:

As·so·ci·a·ted

a.

Joined as a companion; brought into association; accompanying; combined.

[Webster 1913 Dictionary. Patrick J. Cassidy, 1913.]

Appellants thus respectfully traverse the Examiner's improper, albeit convenient, interpretation of the term "associated with" as being in direct contradiction with the specification as well as the commonly-accepted every day meaning of the term.

Further to the above, Appellants have previously also traversed the Examiner's specious patchwork of Feigen, Deo and Le as simply counterintuitive and self-contradictory. More

specifically, the Examiner alleges that Le teaches the measuring by a trusted device associated with the transaction terminal after the last restart of the transaction terminal at col. 9 ll. 1-48 (microcontroller as trusted device that measures integrity of the bios following a reset) and that Deo discloses allowing financial transaction data to be input into the transaction terminal if it is identified as a trusted terminal, and then puzzlingly announces that it would have been obvious to the skilled person to utilize Deo's method of trust with financial terminals and Le's method of measuring integrity with Feigen's integrity verification system "because it offers the advantage ensuring that sensitive financial information does not fall into the wrong hands." Appellants respectfully contend that this explanation falls rather short. Erstwhile, if Feigen does not teach the terminal being a financial terminal (as per the Examiner at page 4, section 8), then why would the skilled person practicing Feigen be motivated to look at Deo in the first place? What motivation is there *on the face of Feigen* to look at Deo's teachings? All the Examiner has offered is that Deo allegedly teaches "the advantage ensuring that sensitive financial information does not fall into the wrong hands" - which only begs the reverse question, namely if Feigen does not teach financial terminals, then why would the alleged advantage offered by Deo be of any interest to the skilled person practicing Feigen? In other words, *where on the face of Deo* is there any motivation to apply the teachings of Feigen? Appellants submit that the Examiner's proffered motivation is little more than a strained attempt, informed completely by hindsight and not at all by the actual teachings of Feigen and Deo, to pick and choose disjointed bits and pieces of these documents and force them into something superficially akin to the claimed invention but which finds no reasonable support in the prior art nor in common sense.

Further to the above, Appellants had noted that using Le's method of measuring integrity with Feigen's integrity verification system is not only not complimentary in the least bit, but actually is completely redundant. If Le teaches a method of measuring integrity, why would the skilled person go looking to Feigen's integrity verification system? The Examiner's proffered motivation (once again) makes no sense – if Le teaches the desirability of providing reduced system cost, greater system reliability, and assurances that the BIOS is not corrupted, then – again – why would Feigen be consulted? Where does Feigen teach that his system provides these benefits? And, for that matter, since Le teaches that his system provides the aforementioned

benefits, why would anyone go looking elsewhere for these very same benefits? The Examiner offers no reply to this in the present Action.

Furthermore, Appellants previously noted, the Examiner's assertion of the obviousness of combining these three references is devoid of any hint or suggestion as to how exactly the skilled person would go about utilizing Deo's method of trust with financial terminals and Le's method of measuring integrity with Feigen's integrity verification system, and thus sets forth not one iota of the expectation of success required for a proper §103 rejection.

Le teaches the sharing of ROM between two processors, wherein one of the processors measures a checksum of the ROM to establish whether the *data* in the ROM has been corrupted and needs to be replaced. Thus, "the advantage of providing reduced system cost, greater system reliability... and assurances that the bios is usable and non-corrupted" as asserted by the Examiner is only an advantage to an arrangement wherein two processors share ROM. There is absolutely no motivation for a skilled person attempting to practice either of Feigen's method for a head-end verification unit to verify that a remote cable box has not been tampered with, or Deo's method for separate devices to authenticate one another, to look at a reference such as Le that is concerned with allowing two processors to use the same ROM. What does sharing ROM have to do with one unit verifying another, remotely-located unit, or with physically separate, self-contained smart devices being able to authenticate one another? Moreover, there is no teaching in Le of measuring integrity of a device, merely of assessing whether *data* has been *corrupted*.

The Examiner retorts to the above by pointing out that Le also teaches BIOS verification after the startup of a computer, and therefore it is analogous art. This may very well be, but there is still no reasonable expectation of success on the face of the prior art for the skilled person who might be moved to actually attempt to combine these three references in the very specific way imagined by the Examiner, nor does this in any way answer any of Appellants' other contentions - namely that Le is very specifically aimed at a system that includes two processors sharing a single ROM, and that a skilled person would have no reason to consult Le for modifying any system that does not include this unique configuration.

Finally, Appellants asked the simple question – what element in either of Feigen, Le or Deo does the Examiner allege to correspond to the claimed trusted device? That is, a (1) trusted device (2) associated with the transaction terminal and (3) able to measure an integrity metric for the transaction terminal (4) after the last restart of the transaction terminal? "To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success... The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP §2142. As fully set forth above, there is in fact no motivation either on the face of the references themselves nor, logically, in the general knowledge of the skilled person to combine these three references in the disjointed and not-altogether-very-clear manner asserted by the Examiner; even if the combination was attempted, there is certainly no expectation of success on the face of either reference (and the Examiner has made no attempt at even identifying such indication of expected success in either reference, despite repeated explicit requests by Appellants); and, finally, the references do not in fact teach and every limitation of the instant claims.

In view of all of the preceding, Appellants respectfully submit that claims 1, 5 and 8 are in fact patentable over the art on record, and respectfully request that the Examiner be overturned on Appeal and these claims passed to issue.

Claims 2 and 4 are dependent on claim 1, and claim 10 is dependent on claim 8. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claims 1, 5 and 8, Appellants submit that claims 2, 4 and 10 are also allowable.

**Issue 2: Whether claims 3 and 6 are patentable under 35 U.S.C. 103(a) over Feigen, Le and Deo and further in view of U.S. Patent No. 6,694,436 to Audebert (hereinafter "Audebert").**

Claims 3 and 6 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Feigen, Deo and Le in view of U.S. Pat. No. 6,694,436 to Audebert. Claims 3 and 6 depend from claims 1 and 5, respectively. Therefore, in light of the above discussion of claims 1, 5 and 8, Appellants submit that claims 3 and 6 are also allowable at least based on their respective dependencies.

**Issue 3: Whether claim 7 is patentable under 35 U.S.C. 103(a) over Feigen, Le, Deo and Audebert and further in view of U.S. Patent No. 6,772,331 to Hind (hereinafter "Hind").**

Claim 7 stands rejected as unpatentable over Feigen, Deo, Le, Audebert and further in view of U.S. Pat. No. 6,772,331 to Hind. Claim 7 depends from claim 5 and Appellants thus submit that this claim is also allowable at least based on its dependency.

**Issue 4: Whether claim 9 is patentable under 35 U.S.C. 103(a) over Feigen, Le and Deo and further in view of U.S. Patent No. 5,272,754 to Boerbert (hereinafter "Boerbert").**

Claim 9 stands rejected as unpatentable over Feigen, Deo and Le in view of U.S. Pat. No. 5,272,754 to Boerbert. Claim 9 depends from claim 8 and Appellants thus submit that this claim is also allowable at least based on its dependency.

Claims

1. A method for allowing a financial transaction to be performed using a electronic system, the method comprising:

interrogating an electronic transaction terminal with an electronic security device to obtain an integrity metric for the transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal;

determining if the transaction terminal is a trusted terminal based upon the integrity metric; and

allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal.

2. A method according to claim 1, further comprising:

providing user identification data for the user of the electronic security device to the transaction terminal via the security device to allow authorisation of the transaction associated with the financial transaction data.

3. A method according to claim 1, further comprising:

displaying a user secret if the transaction terminal is identified as a trusted terminal.

4. A method according to claim 1, further comprising:

compartmenting different types of transactions into different compartments.

5. A financial transaction system, comprising:

an electronic financial transaction terminal; and

an electronic security device having interrogation means for interrogating the transaction terminal to obtain an integrity metric for the transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal , determining means for determining if the transaction terminal is a trusted terminal based upon the integrity metric, and means for allowing financial transaction data to be input into the transaction terminal if

the transaction terminal is identified as a trusted terminal.

6. A financial transaction system according to claim 5, wherein the electronic financial transaction terminal further comprises a display for displaying a user secret if the transaction terminal is identified as a trusted terminal.

7. A financial transaction system according to claim 6, wherein the user secret is deleted on completion of the financial transaction.

8. An electronic security transaction device having interrogation means for interrogating an electronic financial transaction terminal to obtain an integrity metric for the transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal, determining means for determining if the transaction terminal is a trusted terminal based upon the integrity metric, and means for allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal.

9. An electronic security transaction device according to claim 8, further comprising a switch for initiating the transfer of financial transaction data to the transaction terminal if the transaction terminal is identified as a trusted terminal.

10. An electronic security transaction device according to claim 8, wherein the transaction device is a wireless trusted personnel device.

There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.